RPKI 部署指南（1.0 版）

RPKI Deployment Guide (Version 1.0)

中国互联网络信息中心

中国电信股份有限公司研究院

中国移动通信集团有限公司

中国联合网络通信有限公司研究院

中国科学院计算机网络信息中心

互联网域名系统国家地方联合工程研究中心（ZDNS）

2025 年 10 月

联合编写单位及贡献者

中国互联网络信息中心

杨学、张立坤、刘永祥、孙莺菲、王云飞、张恒、孙从友、胡聪、姜博文

中国电信股份有限公司研究院

解冲锋、刘志华、郑忠民、孙嘉琪

中国移动通信集团有限公司

常诚、刘博、赵玉印

中国联合网络通信有限公司研究院

徐雷、王翠翠、史金雨

中国科学院计算机网络信息中心

李彦彪、邹慧

互联网域名系统国家地方联合工程研究中心（ZDNS）

马迪、邵晴、包卓

目录

前言 1

英文缩写对照表 2

一、 互联网域间路由体系 4

1.1 域间路由体系介绍 4

1.1.1 自治系统 4

1.1.2 域间路由协议 4

1.2 域间路由安全风险 5

1.2.1 路由劫持 5

1.2.2 路由泄露 5

1.2.3 路径伪造 6

1.3 路由劫持风险分析 6

1.4 资源公钥基础设施 7

1.4.1 RPKI 的发展历程 7

1.4.2 RPKI 全球部署现状与趋势 9

1.4.3 RPKI 部署的重要性和紧迫性 10

二、 RPKI 技术体系 11

2.1 基于地址分配体系的 RPKI 架构 11

2.1.1 RPKI 证书签发体系 12

2.1.2 RPKI 证书存储系统 13

2.1.3 RPKI 证书同步验证体系 13

2.2 RPKI 的路由源验证流程 13

2.2.1 证书签发 14

2.2.2 证书存储 16

2.2.3 证书同步验证 16
三、RPKI 总体部署指南 18
3.1 签发主体职责和行动指南 18
3.1.1 签发主体 18
3.1.2 行动路线图 18
3.1.3 行动指南 18
3.2 验证主体职责和行动指南 18
3.2.1 验证主体 18
3.2.2 行动路线图 18
3.2.3 行动指南 19
四、 RPKI 签发指南 19
4.1 签发前准备 20
4.1.1 梳理地址资源 20
4.1.2 模式选择 20
4.1.3 签发优先级排序 21
4.2 ROA 签发流程与规范 21
4.2.1 ROA 内容 21
4.2.2 最大前缀长度设置规范 22
4.2.3 注意事项 22
4.2.4 签发操作步骤 22
4.3 签发数据运维 23
4.3.1 建立常态化管理流程 23
4.3.2 建立分层审计体系 23
4.4.3 组织定期培训 24
4.4 常见问题和案例解析 24

4.4.1 常见问题 24
4.4.2 案例分析 26
五、 RPKI 验证指南 26
5.1 验证部署前准备 26
5.1.1 部署或接入 RPKI 的 RP 26
5.1.2 网络设备配置检查 27
5.1.3 设计路由策略 28
5.2 分阶段启用验证 29
5.2.1 阶段一：监控模式 29
5.2.2 阶段二：部分强制模式 30
5.2.3 阶段三：全面启用模式 30
5.3 运维与监控 31
5.3.1 监控 RP 运行状态 31
5.3.2 监控 RPKI 验证结果 32
5.4 注意事项 33
5.4.1 路由器更新存在延迟 33
5.4.2 采用分阶段部署策略 33
六、 RPKI 的局限性和应对 33
6.1 当前局限 34
6.1.1 对路径劫持与泄露防护的有限性 34
6.1.2 依赖全球分布式系统的完整性和一致性 34
6.2 应对与演进 35
6.2.1 ASPA 技术 35
6.2.2 BGPsec 技术 35
七、结语：共筑可信网络，迈向安全未来 36

部分路由劫持事件.....38

前言

本指南是面向国内网络运营商、安全运维人员及技术决策者的专业化实操手册，聚焦资源公钥基础设施（RPKI）技术在我国网络环境中的落地全流程，旨在为打击互联网中存在的欺诈性路由信息提供标准化、可落地的实施框架。指南系统性地提供 RPKI 部署的全生命周期指导，覆盖从前期规划到后期运维的完整链条，帮助相关组织和个人评估并引入 RPKI 技术对策，有效防范因路由欺诈引发的各类安全问题。本指南是构建可信互联网路由体系、推动 IPv6 网络路由安全建设的关键技术参考文档。

英文缩写对照表

英文缩写	英文全称	中文释义
AFRINIC	African Network Information Centre	非洲网络信息中心
API	Application Programming Interface	应用程序编程接口
APNIC	Asia-Pacific Network Information Center	亚太互联网络信息中心
ARIN	American Registry for Internet Numbers	美国互联网号码注册管理机构
AS	Autonomous System	自治系统
ASPA	Autonomous System Provider Authorization	自治系统供应商授权
BGP	Border Gateway Protocol	边界网关协议
BGPsec	Border Gateway Protocol Security	边界网关协议安全（扩展协议）
CA	Certificate Authority	证书颁发机构
CDN	Content Delivery Network	内容分发网络
CPU	Central Processing Unit	中央处理器
CRL	Certificate Revocation List	证书吊销列表
DDoS	Distributed Denial-of-Service	分布式拒绝服务攻击
DNS	Domain Name System	域名系统
EE	End Entity	终端实体
IANA	Internet Assigned Numbers Authority	互联网号码分配机构
IETF	Internet Engineering Task Force	互联网工程任务组
IRR	Internet Routing Registries	互联网路由注册局
ISP	Internet Service Provider	互联网服务提供商
LACNIC	Latin America and Caribbean Network Information Centre	拉丁美洲和加勒比海地区互联网地址注册机构
LIR	Local Internet Registries	地区互联网注册管理机构
MANRS	Mutually Agreed Norms for Routing Security	路由安全相互协议规范
NIR	National Internet Registry	国家互联网注册管理机构
NIST	US National Institute of Standards and Technology	美国国家标准与技术研究所
RFC	Request for Comments	请求评论（IETF 发布的技术标准文档系列）

RIPE NCC	Reseaux IP Europeens Network Coordination Centre	欧洲 IP 网络协调中心
ROA	Route Origin Authorizations	路由源授权
ROV	Route Origin Validation	路由源认证
RP	Relying Party	依赖方（RPKI 体系中负责同步验证数据的组件）
RPKI	Resource Public Key Infrastructure	资源公钥基础设施
RPKI-RTR	RPKI to Router Protocol	资源公钥基础设施到路由器协议
RRDP	RPKI Repository Delta Protocol	资源公钥基础设施仓库增量协议
RSYNC	Remote Synchronization	远程同步（协议）
SIDR	Secure Inter-Domain Routing	安全域间路由（IETF 工作组）
SRv6	Segment Routing IPv6	基于 IPv6 的分段路由
VRPs	Validated ROA Payloads	已验证的 ROA 有效载荷

一、互联网域间路由体系

1.1 域间路由体系介绍

1.1.1 自治系统

自治系统（Autonomous System, AS）是指互联网中处于一个管理机构控制之下的路由器和网络群组。每个 AS 都被分配了其专属的 AS 号用于区分。通过将互联网划分为多个 AS，能够有效避免全局路由表的爆炸性增长，且将故障隔离在 AS 内部，避免了对其他 AS 的直接影响。各 AS 允许独立定义路由策略，从而提高了系统的灵活性。

1.1.2 域间路由协议

域间路由主要处理不同 AS 之间的路由选择，用到的协议是边界网关协议（Border Gateway Protocol, BGP）。BGP 允许不同的 AS 之间交换路由信息，并根据各自的策略决定数据传输的路径。

BGP 的优点包括一是灵活性和可扩展性，BGP 允许每个 AS 独立地决定其路由政策，这使得它非常适合于互联网规模的路由需求；二是强大的路由策略控制，通过各种属性（如 AS_PATH, LOCAL_PREF 等），网络管理员可以非常细致地控制流量进出自己的网络。

BGP 的缺点包括一是安全性弱，缺乏对路由宣告的验证机制，容易遭受路由劫持等威胁；二是复杂性高，BGP 配置和管理相对复杂，需要深入了解路由策略和网络架构；三是收敛速度慢，与某些域内路由协议相比，BGP 在检测到拓扑变化时的响应时间较长；四是资源消耗大，由于维护大量的路由表和属性信息，BGP 可能消耗较多的内存和中央处理器资源，特别是在大型网络中。

1.2 域间路由安全风险

1.2.1 路由劫持

路由劫持是指某个 AS 通过发布错误的路由信息（例如宣告其并不合法持有的 IP 前缀，或伪造通往某前缀的 AS 路径），从而非法吸引并劫持网络流量的行为。常见的路由劫持种类如下:

- 精确前缀劫持：攻击者宣告与合法前缀完全相同的 IP 地址段，并通过伪造更优的路径属性（如更短的 AS 路径或更高的本地优先级）吸引流量。
- 子前缀劫持：攻击者宣告比合法前缀更具体的子前缀（即更小的 IP 地址范围）。根据 BGP 的最长前缀匹配规则，劫持者的子前缀会优先于合法前缀被选择，导致流量被导向攻击者。
- 伪造起源劫持[1]：攻击者宣告当前未在 BGP 表中活跃或已弃用的合法前缀，利用资源公钥基础设施（Resource Public Key Infrastructure, RPKI）和互联网路由注册表（Internet Routing Registries, IRR）信息更新滞后或不一致的漏洞，将这些“空闲”地址块据为己用，以截获原持有者及其潜在通信对端的流量，或干扰其通信。

1.2.2 路由泄露

路由泄露是指 AS 在传播 BGP 路由信息时，违反了既定的路由传播策略或层级关系，将本不应外泄的路由信息转发给不合适的对等方。例如，一个客户网络误将其从上游运营商学习到的全网路由再通告回另一个上游，从而形成“错误路由通告链”。

[1] rfc9319: The use of maxLength in the Resource Public Key Infrastructure

1.2.3 路径伪造

攻击者在通告的 AS_PATH 中插入或修改 AS 号，将合法前缀包装在虚假路径中，以绕过简单的 Origin 验证并伪造与受害者 AS 的邻接关系，从而更隐蔽地吸引或截获流量。

图 1 显示了从 2022 年 1 月到 2025 年 9 月的各类路由安全事件变化趋势（数据源自 BGPWatch[2]）。劫持类事件总体波动明显，尤其在 2023 年 8 月出现劫持异常高峰（3858 起），原因是伊拉克政府网络（AS208293）主动宣告了社交软件 Telegram 的前缀，用来封锁 Telegram 服务。此外，可以发现路由劫持事件存在季节性波动，但总体呈现增长趋势。

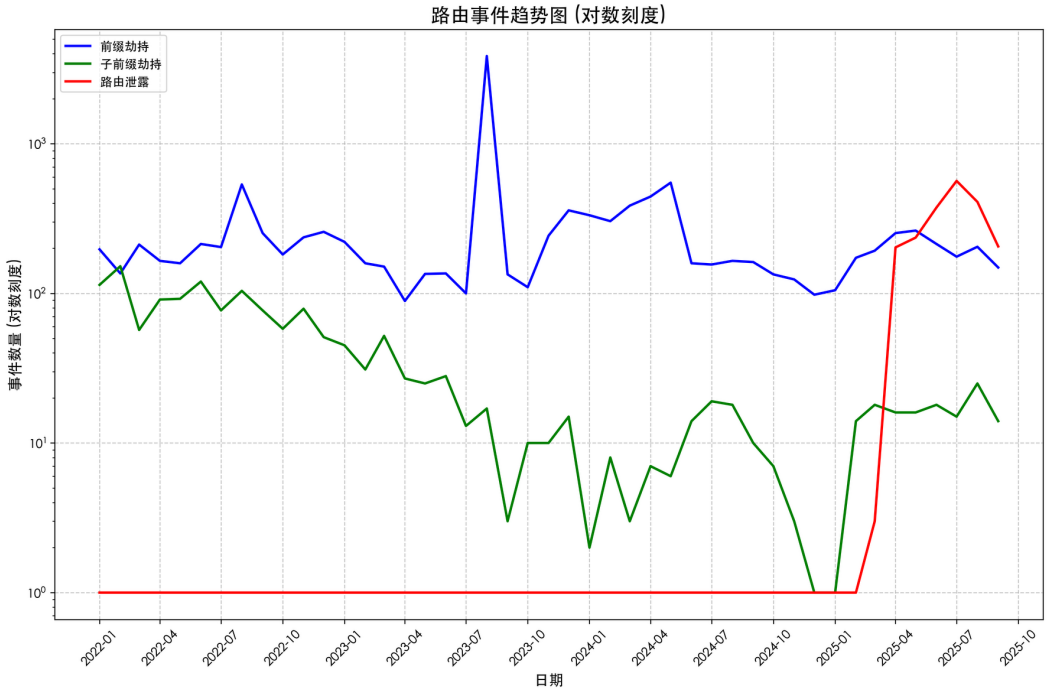

图 1 历年各类路由安全事件变化趋势折线图

1.3 路由劫持风险分析

[2] bgpwatch.cgtf.net

路由劫持因其利用基础协议漏洞、可引发大规模服务中断与数据泄露、具备国家级网络对抗潜力的特点，已成为最具基础性、多发性和战略威胁性的路由安全风险。附件 1 介绍了近年来的重要路由劫持事件，分析这些事件可以发现高影响事件通常具有两个特征：一是“大型网络/骨干或国家级运营商”相关的异常（可承载大量被截流流量）；二是“关键服务（如域名系统（Domain Name System, DNS）、证书机构、金融服务、加密货币服务等）”相关的异常。引发这些事件的原因既有错误配置也有恶意行为，但无论是否恶意，BGP 路由劫持一旦发生，其影响范围可迅速波及全球互联网。

1.4 资源公钥基础设施

RPKI 是一项旨在增强 BGP 安全性的机制，它构建了一种框架体系，使实体能够明确声明其合法拥有的 IP 地址或自治系统（AS）编号，并为其合法持有的 IP 地址和 AS 号的授权提供了完整性和真实性认证保障。这一机制确保了路由信息的可验性，从而增强了整体网络的安全性。

路由起源授权（Route Origin Authorizations, ROA）和路由起源认证（Route Origin Validation, ROV）是基于 RPKI 的最重要且广泛部署的应用之一。通过对 BGP 路由消息的起源真实性进行验证，实现对劫持路由的过滤。此外，RPKI 还可支撑对 BGP 路由消息的路径完整性进行验证（BGPsec 机制）以及对 BGP 路由消息的传播合法性进行验证（ASPA 机制）。

1.4.1 RPKI 的发展历程

2006 至 2007 年，互联网工程任务组（Internet Engineering Task Force, IETF）正式成立“安全域间路由（Secure Inter-Domain Routing, SIDR）”工作组，开始研究通过密码学机制验证互联网路由资源的合法性。

2011 年前后，全球五大区域互联网注册机构（Regional Internet Registry, RIR）陆续参与到 RPKI 的实际部署中。

2012 年是 RPKI 标准化的关键节点。IETF 发布了以 RFC 6480 为核心的一系列标准文档，系统定义了 RPKI 的体系结构、证书层级、信任锚管理机制以及验证逻辑。同年发布的 RFC 6481 至 6493 等多篇 RFC 涵盖了资源证书格式、ROA 签名模板、清单与证书吊销列表（Certificate Revocation List, CRL）等具体实现细节。至此，RPKI 的技术体系框架基本确立。

2013 年，RFC 6810 发布，定义了 RPKI 到路由器的交互协议（RPKI to Router Protocol, RPKI-RTR），使验证结果能够直接传递到路由设备，从而在路由设备层面实现起源验证。

2017 年，RFC 8181 进一步规范了 RPKI 对象的发布流程，确保 RIR、信任存储库和资源持有者之间能够安全、可靠地同步与分发证书与 ROA 对象，提升了系统的可操作性与一致性。

2020 年，IETF 陆续发布了 RFC 8893 与 RFC 8897 等文档，扩展了 RPKI 的应用场景与安全要求。RFC 8893 将起源验证机制引入路由出口策略中，使 RPKI 能够在“出向流量”环节发挥作用；而 RFC 8897 则对信任方软件提出了明确的实现与安全要求，为大规模部署提供了标准化支撑。这一阶段标志着 RPKI 技术由基础架构建设迈入生态完善与优化阶段。

目前，IETF 已启动对部分标准（如 RFC 8210）的修订，以提升 RPKI-RTR 协议的安全性与兼容性，增强路由验证过程的稳定性与可扩展性。

1.4.2 RPKI 全球部署现状与趋势

（1）RPKI 部署数据统计

美国国家标准与技术研究所（US National Institute of Standards and Technology, NIST）运行的 RPKI Monitor、路由安全相互协议规范（Mutually Agreed Norms for Routing Security, MANRS）、NLnet 实验室以及亚太互联网络信息中心（Asia-Pacific Network Information Center, APNIC）持续研究和统计跟踪 ROA 创建动态和 ROV 验证结果。

根据 APNIC 的数据显示，全球超过一半的“在用”IP 地址空间已纳入 RPKI 认证范畴内。截至 2025 年 9 月，在 IPv4 地址空间方面，39.7%的 IPv4 地址显示是未知（unknown）状态，53.6%是有效（valid）状态，6.7%是无效（invalid）状态。在 IPv6 地址空间方面，33.7%的 IPv4 地址显示是 unknown 状态，58%是 valid 状态，8.3%是 invalid 状态。

也就是说，如果路由器强制启用 ROV 过滤（只接受 valid 状态的路由）的情形下，unknown 和 invalid 状态的路由都将被拒收，导致全球接近二分之一的 IP 地址被过滤。

（2）RPKI 部署现存挑战

RPKI 体系在域间路由系统安全以及其他领域的学术研究和应用实践仍然处于起步阶段，面临包括部署开销、可扩展性在内的风险和挑战，包括层级式信任模型

引入的资源认证安全风险、数据分发的效率、人工配置引入的管理风险等。基于现有的研究工作和部署经验，RPKI 体系仍有许多问题需要进一步深入研究和分析。

尽管 RPKI 技术本身及其部署应用还有许多亟待解决的问题，基于 RPKI 为域间路由系统提供安全认证服务仍是大势所趋。如何在充分发挥 RPKI 技术优点的基础上，最大限度地减少由其引入的隐患风险，是研究人员下一步工作需要着手解决的问题。

1.4.3 RPKI 部署的重要性和紧迫性

从安全层面看，RPKI 作为保障互联网基础资源安全的重要机制，其价值不仅体现在防止路由劫持与错误传播，更在于构建可信、可验证的网络信任体系，保障路由系统的安全与稳定运行。在传统 BGP 路由体系中，网络路径的选择依赖信任传播机制，缺乏对 AS 发布路由的真实性验证，这为错误配置、恶意攻击以及前缀劫持提供了可乘之机。任何一起路由劫持事件都可能导致大规模网络中断、通信中断或敏感数据泄露，对政务、金融、电信、能源等国家关键行业产生严重影响，RPKI 的出现有效降低了路由劫持事件发生的可能性。

从战略层面看，RPKI 的部署已成为全球互联网治理的共识与行动重点。APNIC、欧洲 IP 网络协调中心（Reseaux IP Europeens Network Coordination Centre, RIPE NCC）、美国互联网号码注册管理机构（American Registry for Internet Numbers, ARIN）、拉丁美洲和加勒比海地区互联网地址注册机构（Latin America and Caribbean Network Information Centre, LACNIC）、非洲网络信息中心（African Network Information Centre, AFRINIC）五大 RIR 均已全面支持 RPKI 体系建设，全球主流运营商也在持续推进部署。美国政府在 2023 年发布了《加强互联网路由安

全路线图》，将互联网路由系统的安全问题上升到国家战略高度，明确提出要通过推广 RPKI 与 BGP 安全标准、强化运营商合规要求等手段，系统性地提升全球互联网的信任基础。随着国际互联网安全验证机制的普及，RPKI 已逐步成为国际互联的“信任通行证”。未来，缺乏 RPKI 部署的网络可能在互联互通中面临信任缺失、路由受限、可达性下降等风险，甚至被边缘化。

总而言之，路由安全已不仅是技术问题，更是网络主权、关键基础设施防护、国家安全能力的体现。RPKI 的价值不仅在于提升技术安全防护能力，更在于支撑国家网络主权、维护国际互联互信，推动网络基础设施向自主可控、可信可管的方向发展。

二、RPKI 技术体系

2.1 基于地址分配体系的 RPKI 架构

如图 2 所示，RPKI 体系主要包括三部分：证书签发体系、证书存储体系以及证书同步验证体系。其中，RPKI 的证书签发体系与互联网号码资源由上至下的分配架构相对应。RPKI 涉及的所有证书都存放至 RPKI 资料库中供依赖方（Relying Party, RP）同步。RP 同步并验证 RPKI 证书和签名对象，而后将验证结果（IP 地址前缀和 AS 号的绑定关系）下放至 AS 边界路由器指导路由过滤。

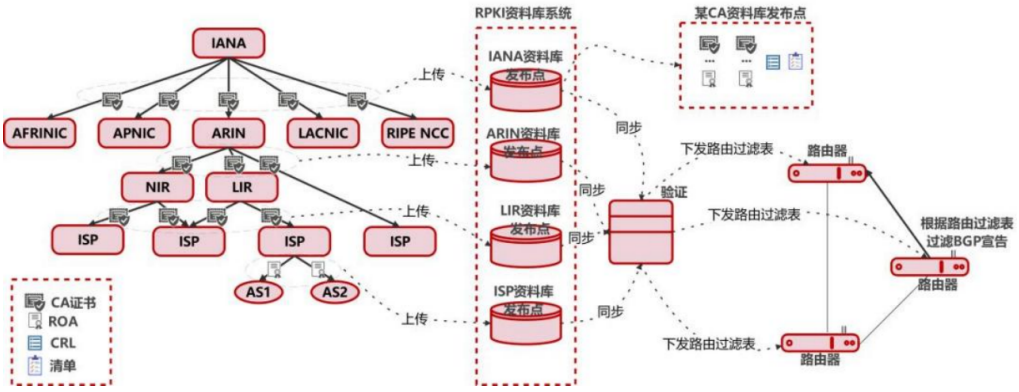

图 2 RPKI 技术架构

2.1.1 RPKI 证书签发体系

RPKI 证书签发体系与现有互联网码号资源分配体系保持一致。顶层节点为五大 RIR，下层节点包括国家互联网注册管理机构（National Internet Registry, NIR）、地区互联网注册管理机构（Local Internet Registries, LIR）、互联网服务提供商（Internet Service Provider, ISP）及其他独立 IP 地址持有者。

RPKI 中的两大证书包括证书颁发机构（Certificate Authority, CA）证书和终端实体（End Entity, EE）证书。CA 证书用来验证 IP 地址空间和 AS 号的持有权，将互联网号码分配机构（Internet Assigned Numbers Authority, IANA）和 RIR、NIR 以及 ISP 关联起来；EE 证书用来验证 ROA 及其他类型的签名对象。

（1）CA 证书

在 RPKI 中，CA 证书的核心作用是对特定实体拥有某段 IP 地址或某个 AS 号的权属进行合法性证明。在 RPKI 资源分配管理体系中，IP 地址分配者和申请者分别对应 IP 地址资源证书的颁发者和持有者。在 IP 地址分配树中，处于树中上游位置的节点不仅承担着分配 IP 资源的角色，同时也负责为其下游节点颁发对应的资源证书。

（2）EE 证书

在 RPKI 中，EE 证书的主要用途是对签名对象（如 ROA 和清单）进行验证操作。当某个 IP 地址资源持有者需要将其拥有的 IP 地址前缀授权给特定 AS 时，需先通过其持有的 CA 证书对应的私钥签发 EE 证书，再使用该 EE 证书对应的私钥生成 ROA，最终 RP（如网络运营商、路由设备）会依据这份 ROA，判断该 AS 是否具备在互联网中合法广播对应 IP 前缀路由的权限。

2.1.2 RPKI 证书存储系统

RPKI 资料库是用来存储证书和签名对象的分布式系统，构成 RPKI 的证书存储体系。在每个 LIR/ISP 的初始化阶段，都需要访问和验证所有的 ROA，并获取所有的资源证书和 CRL 以验证这些 ROA 的有效性，RPKI 资料库用于存储这些证书和签名对象并保证这些证书和签名对象可以被所有的 LIR/ISP 访问、下载。

RPKI 资料库是一个采用分布式存储结构，由很多数据库组成的分布式数据系统，这些数据库被分别部署在相应的注册中心（RIR、NIR、LIR/ISP）上，与每个注册中心相关的资料库至少应该包含由该注册中心签发的所有 CA 证书、EE 证书、CRL 和清单，与 LIR/ISP 等机构相关的资料库还应该包含 ROA。每个 RPKI 资料库都会使用访问控制机制，以确保只有获得授权的实体才可以修改相关信息。

2.1.3 RPKI 证书同步验证体系

RPKI 证书同步验证机制主要由 RP 组成。RP 是指定期获取、解析并对 RPKI 数据对象执行密码学验证的软件组件。RPKI 中的 RP 是连接 RPKI 体系和互联网域间路由系统之间的桥梁，RP 负责从 RPKI 资料库中周期性地同步下载证书和 ROA 并进行验证，从而获得 IP 地址前缀与 AS 号的真实绑定关系，并将这一结果下发给路由器，路由器获得这些数据后用于判断 BGP 路由消息的真实性。

RP 每次验证均从 RIR 开始，并逐级处理所有可发现的发布点。验证完成后，RP 会编译生成已验证的 ROA 有效载荷（Validated ROA Payloads, VRPs），即存储在 ROA 中的“IP 地址前缀-maxLength-AS 号”三元组列表。这些 VRPs 通过 RPKI-RTR 协议传输给 BGP 路由器。

2.2 RPKI 的路由源验证流程

RPKI 的核心价值是通过绑定 IP 地址前缀与 AS 号的合法关系，验证 BGP 路由起源的真实性。其全流程围绕证书签发、证书存储、证书同步验证三个核心环节展开，各环节通过标准化组件与协议协同运作。

2.2.1 证书签发

证书签发是 RPKI 体系的起点，RPKI 采用分层证书体系，通过由上至下逐级颁发资源证书来进行资源授权，证书的内容包含 IP 地址前缀/AS 号与接收机构的绑定关系，最终生成用于路由起源验证的核心对象——ROA。

（1）层级化资源证书分配

如图 3 所示，目前的互联网 IP 地址分配体系形成了一个层级分明的树形结构，全球 RPKI 体系由 IANA 作为根信任锚点，五大 RIR 签发二级证书，一些 RIR 下面可能还存在着第三级的分配机构，比如 NIR 和 LIR，这些机构从上级 RIR 得到 IP 地址前缀和 AS 号，然后留作己用或继续向下级会员分配。

根 CA 向下级 CA 签发 CA 证书，证书中通过 RFC 3779 标准嵌入授权的 IP 地址段和 AS 号范围，证明下级 CA 对特定资源的管理权限，这种层级关系可多级延伸，直至相关资源持有者（如 ISP 等）。资源持有者从上级 CA 获取 EE 证书，该证书明确标注其合法持有资源范围，是后续签发 ROA 的基础。

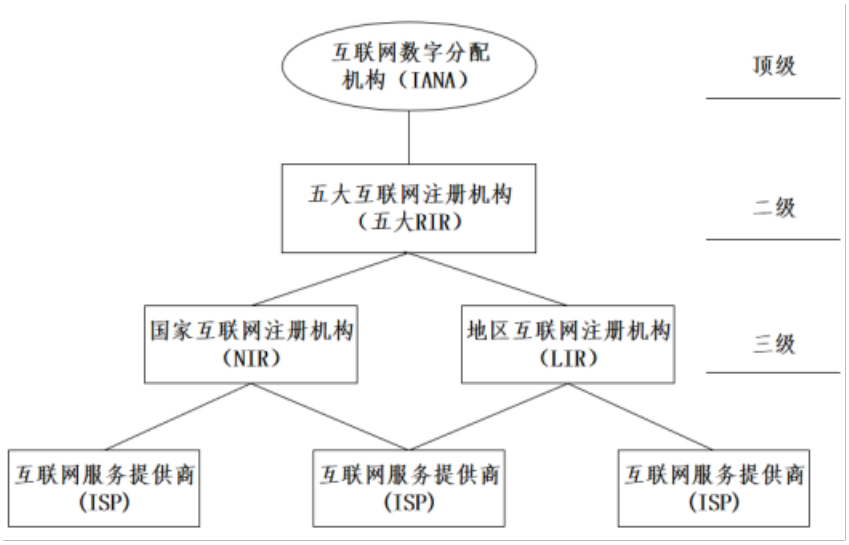

图 3 地址分配树形图

（2）ROA 配置与签发

当资源持有者想授权一个 AS 作为路由起源广播其持有的 IP 地址前缀时，需使用 EE 证书的私钥签发一个 ROA，该 ROA 就可以被用作直接证明“IP 地址前缀-AS 号”的合法绑定关系。

一个 ROA 可以包含多个 IP 地址前缀，但是只能包含一个 AS 号。此外，任何 IP 地址持有者在签发 EE 证书之前，必须有相应的 CA 证书以证明自身是该资源的合法持有者，整个授权过程需要以下 4 个步骤，如图 4 所示。

- 创建 EE 证书，包含需要在 ROA 里授权的 IP 地址前缀信息。
- 组装 ROA 有效载荷，包含“IP 地址前缀-maxLength-AS 号”的合法绑定关系。
- 使用相关 EE 证书的私钥对该 ROA 进行签名，ROA 有效负载是由 CMS 封装的消息组成的。
- 将 EE 证书和 ROA 封装后上传到 RPKI 资料库。

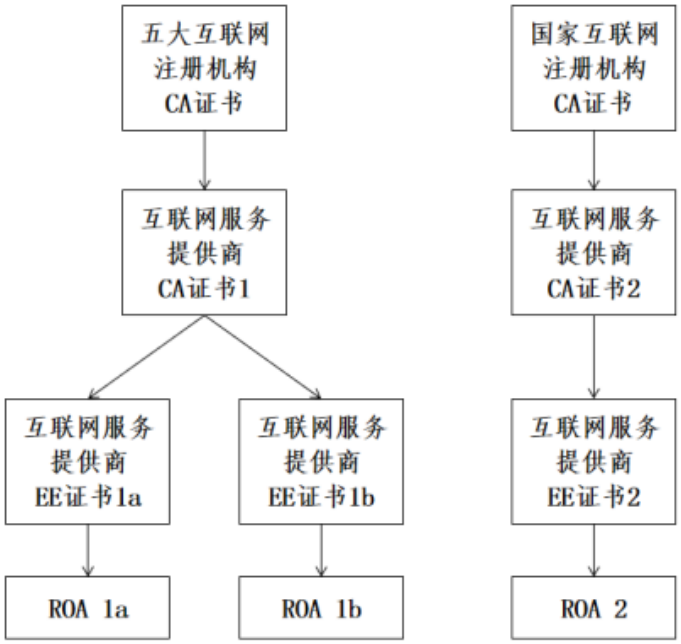

图 4　EE 证书的签发及 ROA 签发

2.2.2 证书存储

RPKI 证书（CA 证书、EE 证书）与 ROA 需存储在公开可访问的 RPKI 资料库中。RP 需要从这些资料库中检索已发布的信息，RFC 8182 提出的 RPKI 仓库增量协议（RPKI Repository Delta Protocol, RRDP）就是用于实现这一检索过程的协议。在 RRDP 协议出现之前，RPKI 资料库通常使用远程同步（Remote Synchronization, RSYNC）协议来实现数据同步，但 RSYNC 协议在面对大量 RP 查询时，服务器需要消耗大量的中央处理器（Central Processing Unit, CPU）和内存资源，且缺乏对缓存基础设施的支持，RRDP 则较好地解决了这些问题。

2.2.3 证书同步验证

证书同步验证同样是 RPKI 发挥作用的核心环节，由 RP 与网络设备协同完成，最终将 ROA 数据对象转换为“可信路由规则”，供 BGP 路由设备选路决策，具体流程分为 3 个阶段：

（1）RP 的数据同步与预处理

RP 核心工作是通过 RSYNC 协议或 RRDP 协议从 RPKI 资料库周期性同步 RPKI 数据，同时验证 ROA 的签名是否与对应 EE 证书匹配、ROA 中声明的 IP 前缀是否在 EE 证书授权的资源范围内，为后续向路由器下发验证依据奠定基础。为了使 RPKI 验证更加高效，IETF 推荐每个 RP 维护一个本地的资料库，这个本地资料库与在线 RPKI 资料库保持同步，所有有效证书、CRL 和其他签名对象都会同步复制过来。

（2）RPKI-RTR 协议的数据下发

RP 通过 RPKI-RTR 协议将验证后的数据下发给边界路由器，具体可参见 RFC 6810 和 RFC 8210。在一个自治网络中，多个 BGP 路由器基于一定的时间周期，向 RP 请求最新的 VRPs。RP 可以直接将 VRPs 数据传送给这些 BGP 路由器，或者可以将验证后的数据传输到 BGP 路由器所在网络的一个缓存服务器，由这个缓存服务器向 BGP 路由器提供数据。

（3）ROV 流程

ROA 中的信息可以用来指导 BGP 路由器工作，相关规定详见 RFC 6483，主要包括以下流程：

- 筛选所有有效的 ROA 记录，留下与目标 IP 地址前缀相同或是目标 IP 前缀的父前缀的 ROA 记录，这一筛选结果构成“候选 ROA 集”。
- 若“候选 ROA 集”为空，则输出“unknown”并退出，否则进行下一步。
- 若“候选 ROA 集”中有任意一条 ROA 能证实该 BGP 消息的真实性（即 ROA 记录中的 AS 号与 BGP 消息的 AS 号相同，且 BGP 消息中 IP 前缀长

度小于等于 ROA 记录中的 maxLength 参数），则输出“valid”并退出，否则进行下一步。

- 输出“invalid”并退出。

三、RPKI 总体部署指南

3.1 签发主体职责和行动指南

3.1.1 签发主体

RPKI 的签发主体是所有 IP 地址资源持有机构，包括所有从互联网注册机构（RIR、NIR 和 LIR）获得 IP 地址分配并进行广播的用户。作为 IP 地址资源所有权人，IP 地址资源持有机构有责任为其广播的 BGP 路由创建相应的 ROA。

3.1.2 行动路线

各签发主体应遵循分阶段、由核心至边缘的渐进式部署策略，优先保障关键基础设施与核心网络受到 RPKI 保护，逐步扩展至全域接入网络。

3.1.3 行动指南

签发主体的具体签发指南见第四章。

3.2 验证主体职责和行动指南

3.2.1 验证主体

RPKI 的验证主体是路由广播单位，包括 ISP、互联网交换中心等。路由广播单位可选择部署 ROV，以增强自身及客户网络的路由安全。同时，接入路由系统的企业及个人用户也应充分认识到 RPKI 验证的重要性，积极关注路由安全威胁，共同提升网络环境的整体安全水平。

3.2.2 行动路线

对于验证主体，验证的行动路线如下:

- 评估现有网络设备（尤其是路由器）对 RPKI 与 ROV 功能的支持情况，必要时进行升级或更换。
- 部署本地 RP 系统或接入商业化 RP 服务，以实现实时路由起源验证。
- 制定清晰的路由安全策略，并分阶段实施，确保平滑过渡和稳定运行。

对于接入路由系统的企业及个人用户，可以采取以下行动:

- 如果不清楚自己的 IP 地址和 AS 号，可以通过在线工具 MANRS 的检测工具[3]进行查询。如果清楚自己的 IP 地址和 AS 号，可以使用在线工具，如 ZDNS 的 RPKI 可视化平台（RPKI Visualization Platform, RPKIVIZ）[4]、Cloudflare 的 RPKI 检测工具[5]、RIPE 的 RPKI 验证器[6]等进行检测，或直接咨询网络服务提供商，确认其是否已启用 ROV。
- 积极敦促并配合运营商为所持有的 IP 地址段（如果 IP 地址属于运营商）正确创建并发布 ROA 记录。
- 若运营多宿主网络，应确保内部网络设备能够正确处理 RPKI 验证状态，避免因无效路由导致业务中断。

3.2.3 行动指南

验证主体的具体验证指南见第五章。

四、RPKI 签发指南

[3] isbgpsafeyet.com

[4] rpkiviz.zdns.cn

[5] rpki.cloudflare.com/?view=validator

[6] rpki-validator.ripe.net

4.1 签发前准备

4.1.1 梳理地址资源

在签发 ROA 前，IP 地址持有机构应当对其持有的各类 IP 地址资源进行分类梳理，明确每种类型的地址段是否需要签发 ROA。

- 正在广播的 IP 地址段：必须签发 ROA，精确匹配当前宣告的前缀、AS 号。当 IP 地址持有机构并不具有 AS 号时，可与相关运营商确认广播 IP 地址段的起源 AS 号的准确性。
- 分布式拒绝服务攻击（Distributed Denial-of-Service, DDoS）防护专用地址段：DDoS 服务提供商在 DDoS 发生时会使用自己的 AS 号广播保护目标的 IP 前缀，在这种情况下，需要预先创建 ROA 以授权服务提供商的 AS 号的建议签发 ROA。
- 未使用/保留地址段：不建议签发 ROA，避免被伪造子前缀劫持利用[7]；如需签发，必须严格限制 AS 号范围，或者为其签发 AS0 ROA。
- 过渡期地址段：需为新老地址段同时签发 ROA，可设置明确的过期时间（notAfter），仍建议过渡期结束后，手动删除签发的老 ROA。
- 特殊用途地址段：根据具体用途决定是否签发 ROA，如 Anycast 节点需为所有宣告 AS 签发 ROA；如 IP 地址用于云服务时，即由云服务提供商宣告自己的 IP，需要创建 ROA 并且制定云服务提供商的起源 AS。

4.1.2 模式选择

[7] rfc9319: The use of maxLength in the Resource Public Key Infrastructure

RPKI 体系提供两种服务模式：托管模式（hosted RPKI）和委派模式（delegated RPKI）。IP 地址持有机构应结合自身基础设施条件与运维能力进行选择。

- 对于初步部署 RPKI 的组织，建议采用托管模式，即由上级 CA 代为签发 ROA，以降低初期部署和管理的复杂度。
- 若 IP 地址持有机构具备相应技术能力并希望获得更高自主性，则可选择委派模式，即自行运维 CA 系统并独立签发 ROA。在此模式下，可选择使用上级 CA（如 RIR 或 NIR）提供的资料库发布服务，以简化操作流程、提升数据发布可靠性。

4.1.3 签发优先级排序

在部署 RPKI 时，合理的 ROA 签发顺序能够有效提升路由安全管理的效率，并降低因配置不当导致的路由失效风险。

- 核心业务与关键基础设施优先：包括但不限于对外提供服务的业务 IP，金融、政务、医疗等敏感行业的网络基础设施等。
- 优先具体子网，其后聚合前缀：先为具体子网签发 ROA，再为聚合前缀签发 ROA，尽量确保子网 ROA 与聚合 ROA 的授权范围无冲突。

4.2 ROA 签发流程与规范

4.2.1 ROA 内容

- IP 地址前缀;
- 起源 AS 号，用于表示宣告 IP 地址前缀路由的 AS 号;

- 最大前缀长度（maxLength），用于表示授权的起源 AS 可宣告的 IP 前缀的最大长度，该项为可选内容。

4.2.2 最大前缀长度设置规范

所有 ROA 签发都应当遵循最小授权原则[8]，即仅包含当前授权 AS 在 BGP 中实际宣告的 IP 前缀，不包含其他任何 IP 前缀。原则上，IP 地址持有者机构应避免在 ROA 中使用 maxLength 属性，因为该属性的使用通常会导致 ROA 不符合最小化原则。当 maxLength 设置过小时，将导致合法路由被判定无效，进而导致网络不可达；当 maxLength 设置过大时，将导致过度授权，使得 ROA 授权前缀仍然存在遭受伪源子前缀劫持的风险。

4.2.3 注意事项

- 创建 ROA 时，一个 ROA 文件只允许配置一个 AS 号，可以配置多个 IP 地址前缀。对于 IP 地址前缀对应多个 AS 号的情况，需要签发多个 ROA 文件来实现。
- 创建 ROA 时，应确保所授权的 AS 号尽可能全面且精准。如存在备用 AS 等需合法宣告该前缀的情形，也应将其纳入签发范围。
- 创建 ROA 时，如出现范围重叠的多个 ROA，它们将同时生效，彼此之间不存在优先级关系，后签发的 ROA 不会取代先前已签发的 ROA。

4.2.4 签发操作步骤

[8] rfc9319: The Use of maxLength in the Resource Public Key Infrastructure

使用 APNIC[9]、RIPE NCC[10]、CNNIC 等不同的 RPKI 平台签发的时候，请参考其签发操作手册。

4.3 签发数据运维

4.3.1 建立常态化管理流程

通过将 ROA 维护嵌入日常网络运维流程，可有效避免因路由声明与 RPKI 验证结果不一致而引发的业务中断风险。建议常态化在签发平台上、或第三方验证软件上（如 Cloudflare[11]、RIPE[12]等）上持续监控与管理 ROA。

当发生以下任一情况时，应在执行 BGP 配置变更的同时，完成相应 ROA 记录的更新:

- IP 地址段的申请或回收;
- BGP 路由宣告策略调整（如新增或撤销起源 AS）;
- 上游运营商或对等互联关系变更;
- 实施 DDoS 防护等特殊路由策略。

若通过多个运营商的多个 AS 号广播同一 IP 地址段，建议建立定期沟通与核查机制，密切关注各运营商发布的 AS 号变更或路由策略通知，确保及时获取信息并修正可能出现的 ROA 异常，避免因信息不同步导致路由失效。

4.3.2 建立分层审计体系

[9] https://www.apnic.net/community/security/resource-certification/certification-practice-statement/

[10] https://www.ripe.net/publications/docs/ripe-540/

[11] rpki.cloudflare.com/?view=validator

[12] rpki-validator.ripe.net

为确保 ROA 管理的持续合规与安全，建议建立定期审计机制（建议每月一次）验证 ROA 授权内容与实际宣告路由的一致性。可采用分层审计体系，实施三级检查机制：第一级为实时监测，进行 7×24 小时不间断检测，如发现 ROA 未签发、AS 号明显冲突，及时通过短信或邮件发送异常告警；第二级为周度检查，比对 ROA 与 BGP 宣告、IRR 记录的差异，识别 maxLength 设置过大的 ROA、冗余 ROA 等异常，生成 ROA 与 BGP 宣告一致性报告；第三级为深度审计，结合人工验证和第三方审计评估，形成系统性改进建议。

4.4.3 组织定期培训

为确保 ROA 签发和维护工作的规范性和有效性，必须对网络运维团队开展系统化的培训。培训内容应涵盖 RPKI 技术原理、ROA 操作规范以及常见问题处置方法，使运维人员能够正确理解 RPKI 在路由安全中的作用，并掌握 ROA 全生命周期管理的实操技能。

4.4 常见问题和案例解析

4.4.1 常见问题

（1）应该选择托管模式还是委派模式?

对于刚开始部署 RPKI 的组织，建议采用托管模式，这种方式由上级认证机构管理 CA，适合缺乏自有 CA 运维能力的机构。如果选择委派模式，建议使用父 CA 提供的资料库发布服务来简化操作。

（2）应该为哪些 IP 前缀创建 ROA?

理想情况下，ROA 应该精确匹配当前在 BGP 中宣告的前缀和 AS 号组合，不要包含未使用的地址段。但在 DDoS 黑洞防护等特殊场景下，可能需要为未在 BGP 中宣告的前缀创建 ROA。

（3）maxLength 字段应该如何设置？

maxLength 是 ROA 中的可选字段，表示授权源 AS 可以宣告的 IP 前缀的最大长度。建议尽可能不使用该字段，而是创建多个精确的 ROA 条目。如果必须使用，要确保其覆盖所有实际宣告的子前缀，否则可能面临子前缀劫持风险，具体参见 RFC 9319。

（4）如何签发重叠前缀的 ROA？

当存在重叠前缀宣告时，应该按照从具体到聚合的顺序创建 ROA：首先为最具体的子前缀（如/24）创建精确授权，然后再为聚合前缀（如/22）创建 ROA。

（5）没有自有 AS 号的组织如何操作？

如果 IP 前缀是由上游提供商代为宣告的，在创建 ROA 时应使用上游提供商的 AS 号作为 Origin AS。

（6）为什么需要定期审计 ROA？

定期审计可以确保 ROA 与当前 BGP 宣告保持一致，发现并清理已不再使用的“僵尸 ROA”，检查是否存在配置错误（如不恰当的 maxLength 设置），这些都是维持 RPKI 系统有效性的关键措施。

（7）密码学无效的 ROA 会导致路由失效吗？

密码学无效的 ROA（如签名验证失败）会被 RPKI 的 RP 直接丢弃，不会影响路由状态。只有当有效的 ROA 明确拒绝某条路由（如前缀被未授权 AS 宣告或超出 maxLength 限制）时，才会导致路由被标记为无效。

4.4.2 案例分析

2025 年 3 月 18 日北京时间 17:30:15，APNIC 为朝鲜签发了一个新的 ROA。新签发的 ROA 将 maxLength 设置为/22，而朝鲜唯一的互联网服务提供商 Star JV（AS131279）实际宣告了四个/24 长度的路由，ROA 致使这些路由被判定为无效。在该错误 ROA 发布后的数分钟内，多个国际运营商依据严格的 RPKI ROV 机制，开始拒绝接收来自 Star JV 宣告的相关路由，导致其路由传播范围大幅缩减，国家互联网可达性受到显著影响[13]。

五、RPKI 验证指南

5.1 验证部署前准备

5.1.1 部署或接入 RPKI 的 RP

RPKI 的 RP 是资源公钥基础设施的重要组成部分，功能是同步并验证 RPKI 证书和签名对象，并将其处理成 IP 地址前缀与 AS 号的真实授权关系，并下放至 AS 边界路由器，从而指导路由过滤。

RP 的核心任务就是从各 RPKI 资料库同步并验证 RPKI 证书和签名对象，并使用 RPKI-RTR 协议[14]向一个或多个路由器提供结果。这种分离解耦设计，使路由

[13] https://www.kentik.com/blog/north-korea-downed-by-faulty-roa/

[14] IETF RFC6810, The Resource Public Key Infrastructure (RPKI) to Router Protocol

器的控制平面不必亲自同步所有 RPKI 资料库发布点并处理繁重的解密和验证工作，极大的减轻了路由器的负担。

RP 的选择与部署是实施 RPKI 验证的第一步。当前流行的 RP 有些还在不断升级，目前主流的开源 RPKI RP 有 Routinator、OctoRPKI、FORT 和 RPSTIR2 等。

RP 系统的架构选择，涉及网络运行机构的路由控制策略、安全保障策略和地址分配策略，需要统筹网络规模、拓扑结构、互联互通策略以及地址资源分配格局等要素。选择一个既可以处理 RP 系统功能诉求的“普遍性”问题，又能兼顾自身网络的具体情况的部署架构，是 RPKI 技术在网络运营商、互联网交换中心等网络运行机构落地应用的关键。主流的 RPKI 部署架构有单点集中部署架构、分布式部署架构、云部署架构等。

5.1.2 网络设备配置检查

图 5 支持 RPKI 的路由器设备厂商

Cisco[15]，Juniper[16]，华为[17]，新华三[18] [19]等厂商均发布了支持 RPKI 路由起源认证功能的路由器硬件设备。应确认使用的路由器型号及操作系统版本对 RPKI-RTR 协议和 ROV 策略的支持情况。

[15] https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/217020-bgp-rpki-with-xr7-cisco8000-whitepaper.html

5.1.3 设计路由策略

当前 RPKI 机制是通过验证 BGP 路由的起源来确保路由安全，其在路由器中的路由策略通常基于路由的 valid、invalid 和 unknown 状态来制定。以下是这些状态的判断情况及常见处理策略。

（1）状态判断

valid: 当 BGP 路由通告与相应的 ROA 匹配时，该路由为 valid 状态。即路由的前缀和 AS 号与 ROA 中记录的信息完全一致，或者 ROA 的前缀范围涵盖了路由通告的前缀，且 AS 号相同。

invalid: 包括无效 AS 号和无效地址前缀两种情况。当存在与路由通告前缀相同（或覆盖）的 ROA，但 AS 号不同时，路由为无效 AS 号状态；当路由通告的前缀长度大于 ROA 中规定的最大长度时，路由为无效地址前缀状态。

unknown: 当没有找到与路由通告匹配的 ROA 时，该路由为 unknown 状态。

（2）处理策略

valid 路由：通常会被正常接受并用于路由表的计算和转发决策，并可以提升此路由的权重，使其优先级更高。

---

16 https://www.juniper.net/documentation/us/en/software/junos/release-notes/22.2/junos-release-notes-22.2r1/topics/new-features/feature-descriptions/routing-protocols-4.html

17 https://info.support.huawei.com/hedex/api/pages/EDOC1100363264/AEN0403J/05/resources/software/nev8r10_vrpv8r16/user/vrp/dc_vrp_sec_maintenance_0036.html

18 https://www.h3c.com/en/d_202305/1855614_294551_0.htm

19 https://www.h3c.com/cn/d_202110/1478983_30005_0.htm

invalid 路由：常见的处理策略是降低此路由权重，或者直接拒绝该路由，不将其加入路由表，以防止路由劫持等安全问题。

unknown 路由：处理策略相对灵活，可以根据网络安全需求和管理员配置来决定，可以通过配置将 unknown 路由按默认路由策略处理。

其他路由处理策略可以参考华为[20]、新华三[21, 22]相关设备厂商的参考文档。

5.2 分阶段启用验证

5.2.1 阶段一：监控模式

监控模式主要包括状态记录与影响评估。在该阶段，网络设备需配置为被动监控模式，通过 RPKI 的 RP 获取到 RPKI 数据，对路由进行验证，得到 RPKI 验证结果，但不执行任何过滤策略，目的在于全面收集全网路由的 RPKI 验证结果，为后续策略实施提供数据支撑。具体技术实现如下:

（1）设备配置：在 BGP 进程中启用 RPKI 验证但禁用强制过滤，具体命令参见各家路由器说明文档。

（2）数据采集与分析：根据各家路由器的对外接口协议，从设备系统接口采集：每条 BGP 路由的 RPKI 状态、前缀、AS 路径及验证时间戳等数据信息。构建分析平台，筛选出 invalid 和 unknown 的路由前缀分布、涉及的 AS 号及潜在流量影响范围。

---

[20] https://info.support.huawei.com/hedex/api/pages/EDOC1100362944/AZN04029/05/resources/vrp/dc_vrp_bgp_cfg_30992.html

[21] https://www.h3c.com/cn/d_202504/2406935_30005_0.htm

[22] https://www.h3c.com/cn/d_202503/2380895_30005_0.htm

（3）影响评估指标：重点分析 invalid 路由的数量占比、是否为核心链路前缀、是否承载关键业务流量等。例如，大型运营商、金融行业等关键客户，需要逐一人工检查是否存在验证为 invalid 的情况，如果存在则需要进一步验证是否是 RPKI 数据错误，并进行多轮次核查。

5.2.2 阶段二：部分强制模式

部分强制模式主要包括定向过滤与压力测试。基于阶段一的数据分析，针对高风险前缀或关键业务链路实施定向过滤，同时维持非关键路径的监控模式，以最小化业务影响并验证过滤策略的有效性。技术要点包括:

- 前缀筛选与策略定制：针对关键客户，比如大型运营商、金融行业客户，当已经在阶段一逐一验证过其 RPKI 验证结果均为 valid 或者为 unknown 后，可以对其 AS 号和地址前缀启用 RPKI 过滤。
- 分级验证机制：对不同业务等级的前缀设置差异化策略，如对大型运营商路由启用严格验证，拒绝 invalid 路由，对普通客户路由暂维持监控模式。
- 实时监控与回退机制：部署 BGP 监控工具，实时追踪过滤前后的路由表变化、流量抖动情况。若发现过滤导致路由黑洞，可通过命令回退，并通知运维团队核查 ROA 配置。

5.2.3 阶段三：全面启用模式

全面启用模式主要包括全网 ROV 部署与持续优化。在完成多轮测试验证后，全网设备切换至强制验证模式，对所有 BGP 路由执行 RPKI 验证，并拒绝所有 invalid 路由，同时构建自动化监控与优化体系。技术实施细节如下:

- 全局策略部署：在核心和汇聚路由器的 BGP 进程中全局启用 RPKI 验证，强制拒绝 invalid 路由。
- 冗余与容灾设计：为避免因 RPKI 数据同步延迟导致的临时验证失败，配置 unknown 状态路由的过渡策略，如允许 unknown 路由进入路由表。
- 自动化运维与优化：通过路由器接口获取 invalid 路由，然后分析历史 invalid 路由数据，识别高频误判场景（如新的 AS 号未及时申请 ROA）。此外，结合 BGP 安全事件，动态调整验证策略优先级，持续提升 BGP 网络抗路由劫持能力。

5.3 运维与监控

5.3.1 监控 RP 运行状态

RP 作为 RPKI 体系的核心组件之一，其核心功能是从全球各个 RPKI 资料库同步 ROA、CRL 等 RPKI 数据，并通过验证构建可信数据集。通过监控 RP 运行状态，确保其与全球资料库的同步正常。

同步机制主要基于 RRDP 和 RSYNC 协议实现。其中 RRDP 协议通过通知文件、全量快照文件和增量文件实现高效同步，并支持内容分发网络（Content Delivery Network, CDN）缓存架构以降低服务器负载，是当前推荐的规模化同步方案；RSYNC 协议则通过差异数据传输，一般作为兼容性补充同步机制。主流 RP 可以设置自动定时同步任务，通过 RRDP 和 RSYNC 协议获取 RPKI 数据，然后将验证后的 RPKI 数据通过 RPKI-RTR 协议传输下发到路由器。

监控 RP 的运行状态需建立多维度指标体系，核心包括同步完整性与数据有效性两类指标。同步完整性监控一方面需跟踪 RRDP 的通知文件的 session_id 与

serial 的变化，确保本地数据版本号与资料库的版本一致，从而获取当前最新数据；另一方面，全量快照文件和增量文件中对新增发布的文件提供了哈希值，这样本地下载的文件也计算出哈希值进行比对，从而确保同步数据的完整性。

数据有效性监控则依赖 RP 对 RPKI 数据的快速验证能力，包括自身验证和证书链验证。自身验证根据不同的 RPKI 文件类型，检查 RPKI 数据文件本身的有效性，包括关键项是否存在，格式是否正确等；证书链验证也是根据不同的 RPKI 文件类型，分别校验证书是否得到上级签发、资源是否在上级资源覆盖范围内、吊销列表文件中声明的文件是否已被吊销、资源清单文件列表中的各个文件哈希值是否正确等等。通过证书自身验证和证书链验证，从而综合评判 RPKI 数据文件是否通过了验证。

5.3.2 监控 RPKI 验证结果

ROV 是 RPKI 保障 BGP 起源安全的核心环节，其将路由宣告经过验证后的结果划分为三类状态：valid、invalid 和 unknown。其中，验证结果为 invalid 的路由是监控核心，因其直接关联前缀劫持或配置错误风险——例如某 BGP 宣告的前缀 193.0.24.0/21 对应 ROA 授权 AS 号为 2120，但 RPKI 数据中起源此前缀的 AS 号却为 2121，此时就会触发 invalid 告警。

针对 invalid 验证结果需建立标准化溯源与处置流程：首先，溯源阶段需结合 BGP 宣告的历史记录、传播路径等信息和对应的 RPKI 数据，定位矛盾点，如 ROA 未包含实际宣告的前缀长度。然后，处置流程需遵循“分级响应”原则：对影响核心业务的 invalid 路由宣告，通过路由策略临时过滤掉，对非核心路由则启动人工核查，并进一步根据既定策略以决定接受或拒绝该路由宣告。

5.4 注意事项

5.4.1 路由器更新存在延迟

RPKI 系统的延迟本质上源于“数据同步-缓存更新-路由生效”的链式流程，与 DNS 的递归查询缓存机制有一定相似性。首先，资料库发布新的 RPKI 数据就需要一定时间；其次，RP 定时通过 RRDP 协议或 RSYNC 协议从全球资料库同步 RPKI 数据也存在延迟性，再加上网络传输、资料库负载压力影响，同步时间可能存在波动；并且路由器也是周期性从 RP 通过 RPKI-RTR 协议获取 RPKI 数据，也存在一定的延迟时间。

5.4.2 采用分阶段部署策略

分阶段部署是 RPKI 运维的核心安全原则，其原则是通过“风险隔离-效果验证-逐步放大”的策略规避配置风险。第一阶段为测试环境验证：利用搭建的模拟仿真环境，通过生成的测试 ROA，结合仿真路由器模拟 BGP 宣告，从而彼此结合来验证验证策略（如拒绝 invalid 路由）的配置有效性，确保 ROA 数据的正确性。第二阶段为非核心业务试点：选取边缘业务前缀（如测试网段、非关键客户资源）启用 RPKI 验证，并监控路由与验证状态分布，观测一定时间无异常后再进入下一阶段。第三阶段为核心业务灰度部署：按前缀重要性分批次启用 RPKI 验证，每批次只增加有限的核心路由，且每批次间隔一定时间，确保单点配置失误仅影响局部范围。第四阶段为对错误配置的“快速回滚+影响熔断”机制，当发现路由器中验证结果为 invalid 的路由出现异常，比如占比突增，则立即联动自动化运维平台暂停此条 RPKI 验证操作，或者暂停全局 RPKI 验证操作并切换回传统路由策略。

六、RPKI 的局限性和应对

6.1 当前局限

尽管推进 RPKI 体系部署为 BGP 路由安全提供了至关重要的起源验证机制，但其设计和部署实践仍存在一定的局限性。全面了解这些局限并认知相应的演进方向，对于网络运营商构建深度防御体系至关重要。

6.1.1 对路径劫持与泄露防护的有限性

RPKI 的核心机制是 ROA 与 ROV，通过验证某个 AS 是否有权对外宣告特定 IP 地址前缀，来有效防范路由劫持。然而，RPKI 体系本身并不验证路径的真实性。例如，某恶意 AS 伪造一条看似合法的路径（如将其 AS 号置于某个知名跨国 AS 之前），并对外宣告其拥有该前缀的有效 ROA。由于 RPKI 仅验证起源 AS 的合法性，而无法验证整个 AS 路径是否与实际数据平面转发路径一致，因此网络中仅对起源验证的接收方路由器会认为该路由是有效的，从而导致路径劫持或路由泄露无法被有效识别，攻击者依然可以实施流量窃听或中间人攻击。

6.1.2 依赖全球分布式系统的完整性和一致性

RPKI 的有效性建立在全球所有网络运营商正确部署和维护其 RPKI 基础设施的假设之上。这种分布式信任模型带来了两个主要挑战：首先是依赖全局性，RPKI 的保护效力具有明显的网络效应，即一个网络的安全收益取决于其上游和对等体网络的部署程度，如果关键上游网络未开启验证，或其发布的 ROA 存在错误，则恶意路由仍可能被广泛传播。其次是错误与滥用风险，RPKI 体系的健壮性依赖于所有参与者的操作准确性。证书或 ROA 的错误签发（如过于宽松的 maxLength 设置）、私钥泄露或合法资源持有者签发恶意 ROA，都可能导致合法路由被标记无效或非法路由被放行。

6.2 应对与演进

为克服上述局限，业界正在从技术补充和远期方案等多个维度进行研究和演进，包括自治系统供应商授权（Autonomous System Provider Authorization, ASPA）和边界网关协议安全（Border Gateway Protocol Security, BGPsec）技术。

6.2.1 ASPA 技术

- **优势：**ASPA 提供了一种基于域间商业关系的路径验证解决方案。其工作原理是由客户 AS 创建并签名，明确授权其一个或多个上游服务提供商 AS。该 ASPA 对象被发布到 RPKI 仓库中，通过编码合法的商业关系，为路径验证提供了重要的间接证据，有效补充了 RPKI 在路径方面的验证能力。
- **局限性**：ASPA 机制依赖于运营商内部商业关系的公开披露，并以此构建全局网络拓扑视图来辅助路径验证，该信息也可能被恶意攻击者所利用，从而引入新的潜在安全威胁。

6.2.2 BGPsec 技术

- **优势**：BGPsec 被设计为 RPKI 的远期演进方案，旨在提供端到端的 AS 路径安全验证，即通过对 BGP 更新报文中的 AS 路径进行数字签名，确保路径上的每一个 AS 都已经同意该路由的传递路径，从而从根本上杜绝路径伪造。BGPsec 方案的核心协议标准由 IETF 于 2017 年发布，即 RFC 8205。
- **局限性**：BGPsec 的现网部署面临严峻挑战。首先是性能开销问题，BGPsec 要求路由器对每条更新报文进行密码学签名和验证操作，这对现有设备硬件性能提出了极高要求，收敛速度受到影响。其次，BGPsec 要求沿途的所有网络都部署实施才能取得显著成效，无法匹配单一网络或少数网

络部署所消耗的工作量，网络运营商缺乏部署动力。因此，BGPsec 的大规模商业化部署尚未展开，短期内难以替代 RPKI 的现有地位。

整体而言，在当前复杂的路由安全环境中，不存在可全面抵御所有威胁的单一技术方案。而 RPKI 作为应对危害最广、最普遍的路由起源劫持问题的关键手段，是现阶段技术最成熟、具备实际部署条件的 BGP 安全增强机制。各网络运营商应将 RPKI 部署纳入优先工作，一方面加快完成 ROA 的生成与发布，为路由验证奠定基础；另一方面在边界路由器上推进 ROV 的试点部署，通过实践验证技术有效性，逐步实现规模化应用。

同时，RPKI 并非孤立的安全解决方案，网络运营商需融入整体路由安全战略，与多类技术、倡议协同配合，形成纵深防御能力。首先，积极参与 MANRS 倡议，借助其提供的 RPKI 部署规范、反欺骗过滤方法及跨网协调机制，提升防护的标准化与协同性；其次，注重技术融合，在部署 RPKI 的同时，结合 IRR、IP-Prefix、AS_PATH 过滤等传统路由加固机制，弥补单一技术短板，同时跟踪 ASPA 等新兴技术的标准化进程，增强技术前瞻性；最后，强化运营支撑，建立完善的路由监控和事件响应机制，确保在发生安全事件时能快速定位和处置。

总之，我们应正视 RPKI 的局限性，但这绝不应成为延迟部署的理由。相反，应以 RPKI 部署为核心，积极拥抱如 ASPA 等补充方案，并关注 BGPsec 等远期技术的发展，通过多层次、深度结合的防御策略，系统性提升全球互联网路由基础设施的韧性和安全性。

七、结语：共筑可信网络，迈向安全未来

本指南系统地介绍了 RPKI 的部署与实践。在结束之际，我们希望再次强调：

第一，RPKI 是构建安全、可信互联网基础设施的基石。它并非一项可选项，而是现代网络运营者必须重视的核心安全机制。通过部署 RPKI，我们能从根源上有效抵御路由劫持、流量窃取等恶意行为，为数字经济的发展筑牢信任的根基。

第二，安全的网络环境需要社会各界的共同参与。我们郑重呼吁所有网络运营者——包括互联网服务提供商、数据中心、交换中心、大型企业及内容提供商——积极行动起来，尽快部署 RPKI，履行自身的安全责任，成为互联网安全稳定运行的守护者。同时，我们也鼓励广大民众主动关注和了解路由安全知识，提高对网络风险的辨识能力，这既是保护自身数字权益的重要一环，也是推动形成全社会共同维护网络安全氛围的关键力量。

第三，互联网安全技术的演进永无止境。RPKI 为我们解决了路由起源验证的问题，而未来的征程在于路径验证。我们展望如 ASPA、SRv6 等新技术的成熟与广泛应用，它们将与 RPKI 形成协同互补，构建一个从起源到路径的完整信任体系。让我们携手推进各类安全技术的融合落地，共同提升我国互联网的整体安全水位，为建设网络强国贡献力量。

行动始于当下，安全成就未来。让我们从部署 RPKI 开始，共同迈向一个更坚韧、更可信的互联网。

目前，我们正持续对本指南进行补充与优化。若您有任何意见或建议，欢迎通过 sunyingfei@cnnic.cn 与我们联系。

附件 1

部分路由劫持事件

2008 年 2 月 24 日，巴基斯坦电信误操作导致全球范围 YouTube 被劫持。为在国内屏蔽 YouTube，巴基斯坦的 ISP（AS17557）声明了 YouTube 的 IP 前缀，且其上游运营商把该操作传播到全球，造成大量地区访问 YouTube 被误导，直到上游撤销路由。

2017 年 1 月，伊朗国家通讯社(TIC)发布了长达 28 小时的虚假 BGP 路线广告，以封锁 256 个外国成人网站。

2017 年 4 月 26 日，俄罗斯运营商 Rostelecom 路由泄露影响金融与支付服务。事件中 Rostelecom 在几分钟内声明了一批金融与在线支付服务（如部分 Visa/Mastercard、支付处理服务、证书机构等）的前缀，导致这些关键服务流量短时通过其网络。

2018 年 4 月 24 日，Amazon Route 53 相关 BGP 遭劫持，导致加密货币被盗。攻击者通过 BGP 劫持把若干 Route 53 相关 IP 路由错误指向恶意服务器，导致部分用户访问被替换/仿冒的 DNS，进而被诱导向假网站输入私钥。

2018 年 11 月 12 日，意外路由泄露导致 Google 部分流量被错误路由导向错误目的地，对网络造成短时影响。Google 表示事件是意外错误配置而非有针对性的攻击。

2019 年 6 月 24 日，Verizon 路由泄露引发大范围故障，影响 AWS 与其他云服务。事件中 Verizon 的 BGP 路由泄露把不当的路由传播出去，导致 Cloudflare 客户站点出现访问缓慢或不可达问题，也波及部分 AWS 服务连接。

2020 年 4 月 1 日，Rostelecom 疑似劫持 Google 与 AWS 的流量。事件中俄罗斯运营商 Rostelecom 宣告或操作了针对 Google 和 AWS 的 BGP 劫持，使部分对应流量被引导至其网络。

2022 年 9 月 25 日，黑客通过 BGP 劫持了 256 个亚马逊 IP，劫取 168 万美元加密资产。事件中，攻击者劫持了 256 个属于亚马逊的 IP 前缀，以 BGP 攻击方式重定向流量，诱导用户访问恶意节点，从而盗走约 168 万美元的加密货币。

2024 年 1 月 5 日，西班牙 ISP Orange 遭劫持 AS 号，并因无效 RPKI 配置导致 3 小时中断。事件中，西班牙 ISP Orange 出现其 AS 号被劫持或路由被不当接管的情况，同时其 RPKI 配置存在失误（无效或错误的 ROA/ROV），导致服务中断约 3 小时。

2024 年 6 月 27 日，Cloudflare 遭遇 BGP 劫持与路由泄露，影响其 DNS 服务 (1.1.1.1)。事件中 Cloudflare 的公共 DNS 解析器 1.1.1.1 遭遇一起组合型事件。既有 BGP 劫持也有路由泄露，造成互联网服务在 300 多个网络、70 多个国家的不稳定。

中国互联网络信息中心

地址：北京市丰台区汽车博物馆西路
9 号院 4 号楼

邮政编码：100070

联系电话：010-59116459

网址：https://www.cnnic.net.cn

中国互联网络信息中心
(CNNIC)